

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

2016

UNITED STATES OF AMERICA,

)

v.

)

Criminal No: 1:16-mj-406

ANDREW OTTO BOGGS
(a/k/a "INCURSIO")

)

&

)

UNDER SEAL

JUSTIN GRAY LIVERMAN
(a/k/a "D3F4ULT")

)

Defendants.

)

**AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT
AND ARREST WARRANTS**

I, BJ Kang, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Washington Field Office ("WFO"), Washington, D.C. I have been employed by the FBI as a Special Agent since 2005. During that time I have participated in numerous investigations of fraud relating to the securities markets, including market manipulation, insider trading, and Ponzi schemes, and I have conducted or participated in arrests, execution of search warrants, surveillance, debriefings of informants, and reviews of taped conversations and securities trading records. I am currently assigned to the criminal computer intrusion squad of the FBI WFO where I investigate crimes involving computer intrusions. Prior to my assignment to WFO, I was a Supervisory Special Agent at FBI Cyber Headquarters, where I provided support to financially-motivated cyber intrusion investigations. I have also received training in cybercrime investigation

techniques, computer evidence identification, and analyzing and tracing digital currency. As a Special Agent of the FBI, I am authorized to investigate crimes involving fraud, computer intrusion, and other crimes stated under federal law, including Title 18 of the United States Code.

2. I make this affidavit in support of an application for a criminal complaint charging ANDREW OTTO BOGGS (also known as "INCURSIO") and JUSTIN GRAY LIVERMAN (also known as "D3F4ULT") with conspiring to violate numerous federal laws as prohibited by 18 U.S.C. § 371. As described in more detail below, BOGGS and LIVERMAN knowingly and willfully conspired to violate multiple federal laws, including 18 U.S.C. § 912 (False personation of officer or employee of the United States); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. §§ 1030(a)(2)(B), (C) & (a)(3) (Fraud and related activity in connection with computers); 18 U.S.C. § 1038 (False information and hoaxes); and 47 U.S.C. § 223 (Harassing telephone calls).

3. The facts in this affidavit come from my personal observations, review of documents and audio recordings lawfully obtained, information obtained from other agents and witnesses, and my training and experience. Because this affidavit is for the limited purpose of establishing probable cause for a criminal complaint, it does not set forth every fact learned in the course of this investigation.

The Defendants and Co-Conspirators

4. Defendant ANDREW OTTO BOGGS and other members of the Conspiracy not charged herein were members of a Conspiracy that referred to itself as "Crackas With Attitude" or "CWA." The group targeted the personal Internet accounts of senior U.S. Government officials for hacking offenses.

5. Defendant JUSTIN GRAY LIVERMAN joined the Conspiracy to target certain senior U.S. Government officials for hacking offenses.

6. Other members of the Conspiracy, not charged herein, include the following individuals based in the United Kingdom: (1) an identified 17-year-old male known as “CRACKA,” (2) an identified 17-year-old male known as “DERP,” and (3) an identified 15-year-old male known as “CUBED.”

7. The members of the Conspiracy utilized anonymizing software, Twitter, and other social media platforms, and instant messaging applications to communicate with one another, to obtain unlawful access to online accounts, publicize their exploits, and harass their victims. The members of the Conspiracy utilized the following Twitter handles, among others:

Name	Twitter Screen Names
JUSTIN LIVERMAN	@D3F4ULT @BASHTIEN_ @SH1N0D4
ANDREW BOGGS	@INCURSIOSUBTER @GENUINELYSPOOKY
CRACKA	@PORNG0D @PHPHAX @DICKREJECT
DERP	@DERPLAUGHING
CUBED	@FRUITYHAX

8. The Conspiracy utilized a technique known as “social engineering,” accessed and attempted to access victims’ online computer accounts without authorization, obtained personal information, and posted that information on the Internet for the purpose of harassing the victims. The Conspiracy specifically targeted accounts

belonging to senior U.S. Government officials, their family members, as well as individuals perceived to have connections to the U.S. Government. The members of the Conspiracy then posted derogatory and harassing comments on the Internet about the victims and/or contacted the victims via telephone to harass them further.

Manner and Means of the Conspiracy

9. The primary methods of the Conspiracy for infiltrating computer systems to further its unlawful goals can be summarized as follows:

- a. A member of the Conspiracy used anonymizing programs and social engineering techniques to obtain unauthorized and unlawful access to a victim's online account, such as the victim's Internet Service Provider ("ISP") account. A member of the Conspiracy would in most cases change the password for that online account, thereby locking the victim out of the account.
- b. A member of the Conspiracy would in some instances share the access information to a victim's account with other members of the Conspiracy. Using that access information, a member of the Conspiracy would try to obtain unlawful access to other online accounts belonging to the victim, such as web-based email or social media accounts.
- c. A member of the Conspiracy would obtain information from each victim account and post that information to the Internet for the purpose of harassing the victim. In some cases, members of the Conspiracy would make telephone calls or online posts for the purpose of harassing the victim.

Summary of the Conspiracy's Unlawful Activities

10. The Conspiracy targeted senior U.S. Government officials and computer systems belonging to the U.S. Government. The targeted individuals and entities included the following:

- a. In or about October 2015, a member of the Conspiracy obtained unauthorized access to Victim 1's AOL account. The servers for AOL are located in the Eastern District of Virginia. Victim 1 is a senior U.S. Government official who works and resides in the Eastern District of Virginia. Using that access, a member of the Conspiracy obtained unauthorized access to several other accounts belonging to Victim 1 or his/her family members, including accounts for Twitter, Verizon, Norton, and other Internet services. Members of the Conspiracy subsequently distributed via the Internet information obtained through this unauthorized and unlawful access to Victim 1's accounts.
- b. In or about November 2015, a member of the Conspiracy obtained unauthorized access to Victim 2's Comcast ISP account. At the time, Victim 2 was a senior U.S. Government official who worked for a federal law enforcement agency. Using Victim 2's credentials, a member of the Conspiracy obtained unauthorized access to Victim 2's account for the Law Enforcement Enterprise Portal ("LEEP"), which is a U.S. Government computer system that provides law enforcement agencies, intelligence groups, and criminal justice entities with access to resources such as the Joint Automated Booking System ("JABS"), Internet Crime

Complaint Center (“IC3”), and Virtual Command Center/Special Interest Group. The Conspiracy subsequently distributed via the Internet information obtained through this unauthorized and unlawful access to Victim 2’s accounts.

- c. In or about December 2015, a member of the Conspiracy obtained unauthorized access to Victim 3’s Verizon account. Victim 3 is the spouse of a senior U.S. Government official.
- d. In or about December 2015, a member of the Conspiracy obtained unauthorized access to Victim 4’s Comcast ISP account. Victim 4 is a senior U.S. Government official who works for a federal law enforcement agency and resides in the Eastern District of Virginia. The Conspiracy subsequently distributed via the Internet information obtained through this unauthorized and unlawful access to Victim 4’s Comcast ISP account.
- e. In or about December 2015, a member of the Conspiracy obtained unauthorized access to the Facebook account of Victim 5’s spouse. Victim 5 is the CEO of a company that provides services such as intelligence, Cyber, and information technology to government and private sector customers. A member of the Conspiracy also obtained unauthorized access to the LinkedIn account belonging to Victim 5, as well as Victim 5’s Comcast account.
- f. In or about January 2016, a member of the Conspiracy made a false bomb threat on a telephone to the Palm Beach County Sheriff’s Office in West Palm Beach, Florida.

- g. In or about January 2016, a member of the Conspiracy published data of more than 80 officers of the several Miami-area law enforcement agencies. The data, which included names, work phone numbers, emails, and titles, was previously obtained from the LEEP computer system when a member of the Conspiracy unlawfully accessed the LEEP computer system.
- h. In or about January 2016 and continuing to in or about February 2016, a member of the Conspiracy obtained information through unauthorized access to the Department of Justice's ("DOJ") Case Information Management System ("CIMS") application, which is run by DOJ's Civil Division. The Conspiracy subsequently distributed via the Internet information obtained through this unlawful access to the DOJ's Civil Division CIMS application.

The Unlawful Objects of the Conspiracy

11. In conducting the malicious computer activities summarized above and described in more detail herein, members of the Conspiracy, including BOGGS and LIVERMAN, conspired to violate numerous federal statutes. Those statutes include, but are not necessarily limited to, the following:

- a. 18 U.S.C. § 912 (falsely assumes or pretends to be an officer or employee acting under the authority of the United States or any department, agency or officer thereof, and acts as such, or in such pretended character demands or obtains any money, paper, document, or thing of value);

- b. 18 U.S.C. § 1028A (knowingly transfer, possess, or use, without lawful authority, a means of identification of another person during and in relation to a specified felony violation);
- c. 18 U.S.C. § 1030(a)(2)(B) (intentionally access a computer without authorization or exceed unauthorized access, and therefore obtain information from any department or agency of the United States);
- d. 18 U.S.C. § 1030(a)(2)(C) (intentionally access a computer without authorization or exceed unauthorized access, and therefore obtain information from any protected computer);
- e. 18 U.S.C. § 1030(a)(3) (intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States);
- f. 18 U.S.C. § 1038 (engage in conduct with the intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of chapter 40 of Title 18); and
- g. 47 U.S.C. § 223 (makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without

disclosing his identity and with intent to abuse, threaten, or harass any specific person).

PROBABLE CAUSE

The Conspiracy Begins

12. On or about July 17, 2015, CRACKA (using Twitter screen name @PORNG0D) exchanged several Twitter direct messages (“DMs”) with Twitter handle @GENUINELYSPOOKY, an account controlled by ANDREW OTTO BOGGS.¹ In one of these DMs, CRACKA related he had obtained the Social Security Number (“SSN”) of a senior U.S. Government official and “and jacked [his/her] comcast email so i can listen to [his/her] voicemail, look at [his/her] answered calls and missed calls and control whats on [his/her] tv. Nvm, i don’t regret it, fuck the gov.” Later that same day, BOGGS (using Twitter screen name @GENUINELYSPOOKY), asked CRACKA if he “would [...] like to join TeamInncuous?” BOGGS told CRACKA that “We’ll only be hitting governments and security firms. I’m waiting on our logo to be finished before we commence attacks on governments.:).” CRACKA responded, “Sure, I’d love to join :P.”

The Conspiracy Targets Victim 1

13. On or about October 12, 2015, at approximately 1:06 p.m., EDT, Victim 1’s spouse received an email notification from Twitter indicating that Twitter had received a request to reset the password for his/her Twitter account. Victim 1’s spouse

¹ Records from Twitter showed that the @GENUINELYSPOOKY account was created on or about December 27, 2014, from Internet Protocol (IP) address 24.182.73.99. An IP address is a unique string of numbers separated by periods that identifies each computer using the IP to communicate over a network. Twitter records for @GENUINELYSPOOKY from on or about October 2, 2015 to on or about November 11, 2015 show that the @GENUINELYSPOOKY account was frequently accessed from IP address 24.182.73.99 during this period. Information obtained from Charter Communications revealed that IP address 24.182.73.99 during the relevant time period was assigned to ANDREW OTTO BOGGS’s father in North Wilkesboro, North Carolina, with whom BOGGS lived.

had not requested that his/her Twitter account password be reset. On the same day, Victim 1's spouse received another email notification from Twitter regarding an unusual login attempt from an unusual device or location as well as a notification that the password to Victim 1's spouse's Twitter account had recently been changed. Moreover, later in the day, Victim 1's spouse received a message on Victim 1's spouse's smart phone that he/she was being followed on Twitter by someone with the Twitter screen name @PHPHAX. The notification read, "@phphax is now following you!" Victim 1's spouse did not recognize this Twitter screen name, which investigation has shown belonged to CRACKA.

14. On or about October 12, 2015, between approximately 4:24 p.m., EDT, and approximately 4:35 p.m., EDT, BOGGS (using Twitter screen name @GENUINELYSPOOKY) and CRACKA (using Twitter screen name @PHPHAX) engaged in the following DM conversation which your affiant believes refers to Victim 1:

@GENUINELYSPOOKY: I'm going to help you with Owning the [U.S. Government Agency affiliated with Victim 1]. I've been looking for evidence of aliens since Gary.

@PHPHAX: i fucking own this loser, i have just released emails of them admitting to torture.

@GENUINELYSPOOKY: If you need any publishing done, let me know. I'll go Charlotte and use public wifi to publish the stolen information.

@PHPHAX: that sounds great :)

15. On or about October 12, 2015, Victim 1's spouse received an email notification from Verizon indicating that there was an update to Victim 1's Verizon account. The email stated, "As a result of your recent contact with Verizon through our call center, our automated phone system or our website, we have updated your account to

add or change your online password and/or reset your Verizon online account.” Neither Victim 1 nor Victim 1’s spouse had requested that the Verizon password be reset. Records obtained from Verizon included October 11, 2015 voice recordings from multiple calls by CRACKA who impersonated a Verizon employee and Victim 1 to gain unauthorized access into Victim 1’s Verizon ISP account.

16. On or about October 13, 2015, Victim 1’s spouse received an email notification from AOL that the password to his/her main AOL account had been reset. The servers for AOL are located in the Eastern District of Virginia. In addition, the alternate email address for Victim 1’s spouse’s AOL account was changed to an email address associated with Twitter screen name @PHPHAX. This email address was unfamiliar to Victim 1’s spouse and which Victim 1’s spouse did not authorize. Because of the unauthorized password reset, Victim 1’s spouse was unable to access his/her AOL email account.

17. On or about October 12, 2015, CRACKA (@PHPHAX) publicly posted on his Twitter page an image of what appears to be a screenshot of Victim 1’s AT&T wireless telephone bill.

18. On or about October 13, 2015, CRACKA (@PHPHAX) publicly posted on Twitter an image of what appears to be a screenshot of Victim 1’s AOL account. CRACKA (@PHPHAX) tweeted, “Its now just a battle between me and [U.S. Government Agency], they keep taking the account back and I keep taking it back after xD.”

19. Between on or about October 13, 2015, and on or about October 18, 2015, Victim 1 received multiple telephone calls to Victim 1’s home and cellular telephones

from CRACKA and/or others. Victim 1 works and resides in the Eastern District of Virginia. The calls were harassing and derogatory in nature. During this period, other family members of Victim 1 located within the Eastern District of Virginia also received telephone calls from CRACKA and/or others which were harassing in nature. For example, on one occasion, CRACKA and/or others allegedly stated to Victim 1 that “we have totally taken over your email account again.”

20. On or about October 14, 2015, at approximately 7:21 p.m., EDT, BOGGS (using Twitter screen name @GENUINELYSPOOKY), sent CRACKA (@PHPHAX) a DM that read, “Hacked anymore [U.S. Government Agency] agents? :P.” CRACKA (@PHPHAX) replied that he had not hacked anymore [U.S. Government Agency] agents and that CRACKA had a one hour phone call with the New York Times regarding the compromise of Victim 1’s AOL account. At approximately 7:44 p.m., EDT, CRACKA (@PHPHAX) sent BOGGS (@GENUINELYSPOOKY) a DM that read, “oh, also, [Victim 1] gets a 17% discount from [Victim 1’s] ATT bills ...” At approximately 9:03 p.m., EDT, BOGGS (@GENUINELYSPOOKY) replied, “That’s not fair.”

21. On or about October 19, 2015, BOGGS (using Twitter screen name @INCURSIOSUBTER) exchanged group Twitter DMs with CRACKA (@PHPHAX) and DERP (@DERPLAUGHING) regarding Victim 1. In these messages, BOGGS and DERP offered their assistance to CRACKA “with whatever we can help with.” BOGGS stated, “I want to carry on [CRACKA’s] legacy if or when he is arrested. I know he’ll receive a harsh sentence because our government doesn’t like being embarrassed, so there’s no better way of protesting than hacking and leaking more documents over and over again.” CRACKA then provided BOGGS and DERP with personal information

belonging to Victim 1 and his/her spouse that included home address and telephone number, cellular telephone numbers, Victim 1's spouse's SSN, U.S. Passport number, email accounts, WiFi password, Media Access Control ("MAC") address,² and several Twitter links to screenshots (partial redaction on some of screenshots) with the following descriptors:

"A little bit of [Victim 1's] Contact list on [Victim 1's] email."

"A screenshot of a email sent to [Victim 1] on [Victim 1's] email."

"A screenshot of [Victim 1's spouse's] Amazon jacked."

"A screenshot of [Victim 1's spouse's] Verizon account jacked."

"Proof of jacking [Victim 1's] ATT account."

Also, BOGGS requested that CRACKA (@PHPHAX) untag @GENUINELYSPOKY (which BOGGS advised was his personal account) from CRACKA's public tweets about Victim 1, and requested that CRACKA (@PHPHAX) instead tag @INCURSIOSUBTER.

22. On or about October 20, 2015, LIVERMAN (using Twitter screen name @_D3F4ULT) exchanged Twitter DMs with CRACKA (@PHPHAX) in which LIVERMAN congratulated CRACKA for successfully targeting Victim 1³. CRACKA replied that "[Victim 1] got bent lol." LIVERMAN then advised CRACKA to stay safe and "dban any drive you don't need bro." Your affiant understands "DBAN" to refer to

² A MAC address is a unique identifier assigned to network hardware interfaces for communications on a physical network such as Ethernet.

³ Time Warner Cable records for an IP address that was used to access the @_D3F4ULT and @BASHTIEN_ Twitter accounts during the relevant time period revealed the subscriber as Edith Liverman. Open source research revealed that JUSTIN LIVERMAN resided with Edith Liverman during the relevant time period.

“Darik’s Boot and Nuke,” a program that can wipe a computer hard drive so that it is no longer readable.

23. On or about November 1, 2015, CRACKA (@PHPHAX) sent LIVERMAN (@_D3F4ULT) a Twitter DM asking for LIVERMAN’s Jabber⁴ chat handle. LIVERMAN replied by providing CRACKA with his Jabber chat handle.

The Conspiracy Targets Victim 2 and the LEEP Computer System

24. According to information obtained from computer hard drives used by LIVERMAN pursuant to a lawful search warrant, on or about November 1, 2015, LIVERMAN and CRACKA engaged in a Jabber chat session. During this Jabber chat session, at approximately 11:10 a.m., EDT, CRACKA stated, “imma drop [VICTIM 2’s] last 4 ssn lol.” At the time, Victim 2 was a senior U.S. Government official who worked for a federal law enforcement agency. LIVERMAN replied, “dooo ittttt.” LIVERMAN told CRACKA that he was located in Key West, Florida, “ducking the miamipd.” Around 3:28 p.m., EDT, CRACKA told LIVERMAN that he was in VICTIM 2’s ISP account which is supported by Comcast records. CRACKA also told LIVERMAN that Victim 2’s spouse paid the bills for the ISP account. Around 3:38 p.m., CRACKA sent LIVERMAN a link to a screen capture tool called LightShot. Your affiant understands LightShot to be a program that allows a user to take a customizable screenshot of any area on his/her desktop. The LightShot link CRACKA sent to LIVERMAN appears to be a screenshot of Victim 2’s monthly Comcast Xfinity bill that is partially redacted. The monthly Comcast Xfinity bill lists VICTIM 2’s spouse’s name. At approximately 3:48 p.m., EDT, LIVERMAN told CRACKA to “plz jack all [Victim 2’s] shit haha.”

⁴ Jabber is a free online instant messaging service.

CRACKA told LIVERMAN that Victim 2 maintained a list of 200 contacts on the account. Around 4:13 p.m., EDT, LIVERMAN told CRACKA, “if you could get into [Victim 2’s] [U.S. Government Agency] acc im sure it would yield.” At approximately 4:21 p.m., EDT, LIVERMAN asked CRACKA “how hard u think itll be to get into [Victim 2’s] [U.S. Government Agency] email acc?” A few minutes later, LIVERMAN stated that he never accessed the U.S. Government Agency’s email servers, but that it “would be nice.” At approximately 4:42 p.m., EDT, CRACKA shared with LIVERMAN information about Victim 2’s Internet connection, specifically Victim 2’s MAC address. Comcast records for Victim 2’s Comcast Xfinity account shows the same MAC address as the one CRACKA shared with LIVERMAN. At approximately 4:48 p.m., EDT, CRACKA sent LIVERMAN a LightShot link to an image of Victim 2’s son.⁵

25. On or about November 1, 2015, at approximately 6:02:14 p.m., EDT, BOGGS (using Twitter screen name @INCURSIOSUBTER) sent CRACKA a Twitter DM asking, “What account did you hijack? I wish I could get involved with hacking and programming for CWA. :(.” Approximately 27 seconds later, at 6:02:41 p.m., EDT, CRACKA replied via DM, “2nd highest person for [U.S. Government Agency];).” Approximately seven seconds later, at 6:02:48 p.m., EDT, CRACKA sent another DM to BOGGS with Victim 2’s full name. Approximately 11 seconds later, at 6:02:59 p.m., EDT, CRACKA sent another DM to BOGGS that read, “200 email contact list.” At approximately 6:03:31 p.m., EDT, BOGGS replied via DM, “Nice.”

⁵ On or about November 30, 2015, LIVERMAN (using Twitter screen name @_D3f4ult) publicly tweeted this image of Victim 2’s son along with the following message: “Daaaaaaad, our @comcast internet is down again!”

26. On or about November 1, 2015, at approximately 8:21 p.m., EDT, LIVERMAN (using the Facebook account Joseph Markowicz⁶) posted on Facebook, “damnit [Victim 2’s spouse’s first name], i thought i told you to pay that bill from @Cisco?! – [Victim 2’s full name], [senior government official] of [U.S. Government Agency] lololol @phphax.” Moreover, on or about November 2, 2015, at approximately 12:19 a.m., EST, LIVERMAN (using Twitter screen name @_D3F4ULT) publicly tweeted, “When you’re [senior government official] of [U.S. Government Agency] but your wife still pays for the internet @PHPHAX,” along with a screenshot, showing what appears to be a redacted version of a Comcast Xfinity payment dated September 7, 2015 for Victim 2’s Comcast account. This is the same screenshot described above in paragraph 23.

27. Computer hard drives used by LIVERMAN contained what appears to be contemporaneous Bandicam⁷ video recordings of some of his actions in relation to the Conspiracy. On or about November 2, 2015, LIVERMAN and CRACKA engaged in a Jabber chat session regarding Victim 2’s cell number. LIVERMAN asked, “...is that realy [Victim 2’s] cell?” CRACKA replied, “yes lmao” and that CRACKA was calling people in Victim 2’s call logs. CRACKA also related, “[Victim 2] fucking regained access to [Victim 2’s] isp hahaha.” LIVERMAN replied, “daaaamn. well you already got access to important shit.” LIVERMAN then told CRACKA that he would

⁶ Facebook records for the Facebook account Joseph Markowicz showed that the registration email address was the same email address that was used to register the Twitter handle @_D3F4ULT. Moreover, the majority of the accesses to the Joseph Markowicz Facebook account for the relevant time period were from the same proxy IP address that was used almost exclusively to access the @_D3F4ULT Twitter account.

⁷ Bandicam is a screen recorder program that can capture anything on a user’s PC screen as high-quality video.

“phonebomb”⁸ Victim 2 if Victim 2’s cell number was legitimate. At approximately 1:42 p.m., EST, LIVERMAN told CRACKA that Victim 2’s cell number was legitimate. According to call records for Victim 2’s U.S. Government-issued cellular telephone, a call that lasted approximately 30 seconds was received at approximately 1:42 p.m., EST, from telephone number (213) 267-XXXX. According to Twitter, telephone number (213) 267-XXXX is a phone number associated with LIVERMAN’s @_D3F4ULT Twitter account. At approximately 1:44 p.m., EST, LIVERMAN related, “when i heard [Victim 2’s] voicemail i fcukkin spit my coffee everywhere.” CRACKA replied, “im forwarding [Victim 2’s] number so whoever calls [Victim 2] gets forwarded to a anti-war number LOL.” LIVERMAN then replied, “waaaittt I wanna do something before that. gonna tell people its my number and to call or text me.” A contemporaneous Bandicam recording dated on or about November 2, 2015 made by LIVERMAN showed him setting up and paying \$20 via Bitcoin for a phonebombing campaign against Victim 2’s Government issued cellular telephone number whereby a call would be placed to Victim 2’s cellular telephone, according to the Bandicam recording, every hour for 30 days. The same contemporaneous Bandicam recording showed LIVERMAN sending by way of a computer application called Guerrilla Mail⁹, the following harassing text message to Victim 2’s Government issued cellular telephone on multiple occasions:

Listen here you fucking boomer, we will destroy your reputation.
Just like [two senior U.S. Government officials, including Victim 1]...

⁸ Phonebombing refers to the act of sending multiple phone calls and/or text messages to a victim cellular telephone number for purposes of harassing the victim.

⁹ Guerrilla Mail is a free disposable email address service. Visitors do not need to register to use the service. Visitors are logged in automatically and a random email address is issued on each visit or they can set their own address.

I guess you couldn't handle us jacking your Comcast ISP accounts
too many times so you actually canceled your account!
And telling me to "watch my back" wasn't a good idea lol
How is your [derogatory comment] [Incorrect spouse name]?
We will keep a close eye on your family, especially your son!

LIVERMAN also included in this message a LightShot link to an image of Victim 2's son. Moreover, at the end of this Bandicam recording, LIVERMAN typed out the following note to himself in Notepad:

fuckin golden

[Victim 2] of the [U.S. Government Agency], [Victim 2's first name and middle initial] fuck cant spell his lastname loooooool

but yeah just boomer incharge on [U.S. Government Agency]

jacked [Victim 2's] comcast isp account, got [Victim 2's] 200 contact list, found [Victim 2's] cell, spammed it via email to sms and now phone bombing [Victim 2] with zeekill threat voicemails lol

28. Moreover, a review of another Bandicam recording dated on or about November 2, 2015, shows LIVERMAN creating an account using Victim 2's name on the so-called darknet market "Abraxas Market," where your affiant know that various illegal items are sold including drugs.

29. During the November 2, 2015, Jabber chat session, LIVERMAN told CRACKA that he wanted to post a message to Facebook soliciting texts and calls to Victim 2's cellular telephone number. At approximately 1:54 p.m., EST, LIVERMAN publicly posted the following Facebook message from his alias account of Joseph Markowicz: "[t]his line will be active for only 24hrs, so call/sms it if you want to talk to me... i also accept sexy nudes lol [Victim 2's Government-issued cellular telephone

number] #AnonSec ./d3f4ult.”¹⁰ Later that same day, at approximately 5:31 p.m., EST, LIVERMAN (using Twitter screen name @_D3F4ULT) publicly tweeted the same message.

30. On or about November 4, 2015, LIVERMAN and CRACKA engaged in another Jabber chat session in which LIVERMAN updated CRACKA on the status of the phonebombing campaign. At approximately 3:32 p.m., EST, LIVERMAN told CRACKA that “if we could get [Victim 2] swatted that would be amazing.”¹¹ Later that day, at approximately 6:05 p.m., EST, CRACKA sent LIVERMAN an image via a LightShot link that appears to be a screenshot of the LEEP computer system login page showing Victim 2’s full name displayed at the top of the page next to the words “Log Out.” LIVERMAN asked CRACKA what information was contained on LEEP, to which CRACKA responded: “every law enforcement info. fucking shaking.” LIVERMAN replied, “holy fucking shittttttt.” LIVERMAN then asked CRACKA if he could search by state/city because “many officers info in miami i would love.” After LIVERMAN reiterated that “i would love a list of officers in miami ;),” at approximately 6:43 p.m., EST, CRACKA sent LIVERMAN by way of Jabber a list of more than 80 officers associated with Miami-area police departments.

31. According to information obtained from computer hard drives used by LIVERMAN pursuant to a lawful search warrant, a file (titled “miami_officers.txt”) on one of LIVERMAN’s hard drives contained the entire dump of information relating to

¹⁰ “AnonSec” is a hacking collective that claims to have hacked over 700 websites. LIVERMAN claims on his @_D3F4ULT Twitter biography to be “A Official Admin of #AnonSec.”

¹¹ Swatting refers to the act of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into dispatching an emergency response based on the false report of an ongoing critical incident.

more than 80 officers associated with Miami-area police departments. Furthermore, on or about November 4, 2015, CRACKA advised LIVERMAN by way of Jabber chat that Victim 2 had not used the LEEP computer system since 2013. A review of Victim 2's internal LEEP access records show that the last time Victim 2 accessed LEEP was in 2013.

32. On or about November 4, 2015, at approximately 7:31 p.m., EST, CRACKA sent DERP (@DERPLAUGHING) a DM that read, "tell incursio to get on cryptocat¹², its fucking insane you wont believe it." At approximately one minute later (7:32 p.m., EST), DERP replied, "Download Wickr¹³ and show me it. You can make your messages delete themselves after a certain you want them to. I'll tell her now though."¹⁴ CRACKA then replied, "tell incursio its insane like INSANELY INSANE." At approximately two minutes later (7:34 p.m., EST), CRACKA sent DERP a DM that read "probably biggest hack ever.."

33. According to Criminal Justice Information Services ("CJIS")¹⁵ and LEEP help desk audio recordings and records maintained by CJIS and LEEP, on or about November 4, 2015, from approximately 6:02 p.m., EST to approximately 7:26 p.m., EST, CRACKA used Victim 2's computer credentials without authorization to access the LEEP computer system. It is believed that CRACKA accessed portions of the LEEP

¹² Cryptocat is an application intended to allow encrypted online chat sessions.

¹³ Wickr instant messaging application allows users to exchange encrypted and content-expiring messages, including photos, videos, and file attachments.

¹⁴ BOGGS represented through private communications with other members of the conspiracy that "Incursio" was a female located in North Carolina.

¹⁵ Access to the LEEP system is maintained by CJIS, which is an FBI organization. Generally, CJIS help desk has the ability to reset passwords for FBI LEEP users.

computer system, including JABS.¹⁶ It is believed that CRACKA queried JABS for the name Jeremy Hammond.¹⁷

***The Conspiracy Releases Information It
Unlawfully Obtained From the LEEP Computer System***

34. On or about November 5, 2015, at approximately 1:30 a.m., EST, DERP (using Twitter screen name @DERPLAUGHING) publicly tweeted, “The @FBI are going to be really embarrassed today/tomorrow. #CWA.”

35. On or about November 5, 2015, at approximately 11:33 a.m., EST, CRACKA (using Twitter screen name @PHPHAX) publicly posted, “34,000 lines of emails, names, position and phone numbers of gov associates, including military. :0 #CWA.” At approximately 11:40 a.m., EST, CRACKA publicly posted, “Just to clear this up, CWA did, indeed, have access to everybody in USA’s private information, now imagine if we was Russia or China.. #CWA.” At approximately 11:50 a.m., EST, CRACKA publicly posted, “Do you guys want a screenshot of what JABS, a federal arrest information tool looks like? We found Jeremy Hammond lol.” Among other tweets, at approximately 3:52 p.m., EST, CRACKA publicly posted, “Happy Nov5 guys! This is only part 1:/Gov/Police/Military names, emails and phone numbers.” This post included links to access this information on two websites, Pastebin.com and Cryptobin.org.¹⁸ The information posted on Pastebin.com comprised approximately 295

¹⁶ JABS is a U.S. government computer system that helps federal law enforcement agencies book, identify, and share information quickly about persons in federal custody. The U.S. Department of Justice developed JABS to support its law enforcement components.

¹⁷ Jeremy Hammond is a convicted computer hacker from Chicago.

¹⁸ Pastebin and Cryptobin are popular websites for storing and sharing text. Though they are used for distributing legitimate data, they also seem to be frequently used as a public repository of stolen information.

pages that listed the names, title, organization, agency, telephone number, and email address of local and federal government officials.

36. On or about November 8, 2015, at approximately 2:21 p.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, “Jeremy Hammond was sentenced to 10 years in federal prison while sabu got off scot-free for his cooperation.” This tweet included what appears to be a screenshot of Jeremy Hammond’s JABS booking report that revealed his arrest photo, date of birth, date of arrest, and other confidential information.

Victim 1’s Personal Information is Released

37. On or about October 21, 2015, WikiLeaks announced that over the coming days it would release documents from Victim 1’s personal email account. Later that day, WikiLeaks released on its website the contents of Victim 1’s personal email account, including highly personal information such as Victim 1’s Standard Form 86 (“SF-86”), and other information to include DOBs, SSNs, contact numbers, and email addresses of individuals employed at law firms and the U.S. Senate.¹⁹ WikiLeaks made additional information from Victim 1’s personal email account available on or about October 22, 2015 and October 26, 2015.

38. On or about November 9, 2015, Twitter user @CthulhuSec²⁰ publicly posted the following tweet: “Thanks to the #CWA/@Fruityhax for providing the files directly. Here is the [Victim 1’s] AOL Email Files: [Victim 1’s Employer].thecthulhu.

¹⁹ SF-86 is entitled “Questionnaire for National Security Positions.” SF-86 is used by the U.S. Government as part of its background investigation process into individuals seeking national security positions. SF-86 contains highly personal information, including social security numbers, dates of births, current and prior addresses, of the applicant as well as family members.

²⁰ The user of @CthulhuSec regularly hosts data on his server that others may have obtained from compromised accounts.

com.” This tweet contained an Internet link to another web site titled, “[U.S. Government Agency] Data Leaks.” This web site contained links to download the personal data obtained from Victim 1’s AOL account, including Victim 1’s SF-86 form, and attributed credit to “the CWA group (@phphax & co).”

The Conspiracy Tries to Regain Access to the LEEP Computer System

39. A member of the Conspiracy continued to try to regain access to the LEEP computer system by posing as Victim 2 and at other times posing as other government officials. Specifically, from on or about November 3, 2015 to on or about December 20, 2015, CRACKA and potentially other individuals called the LEEP help desk approximately 34 times and the CJIS help desk approximately 56 times. These calls were recorded.

40. On or about November 21, 2015, CRACKA and BOGGS exchanged Twitter DMs about regaining access to the LEEP computer system. CRACKA asked BOGGS whether he should “add our aliases when i regain access?” BOGGS responded “Yeah, add our aliases,” and subsequently advised CRACKA to be careful and that he could end up in jail if the authorities attributed his activities back to him.

The Conspiracy Targets Victim 3’s Spouse

41. On or about December 10, 2015, among other things, LIVERMAN and CRACKA engaged in a Jabber chat session about Victim 3’s spouse. Specifically, at approximately 5:17 p.m., EST, LIVERMAN stated, “[Victim 3’s spouse] talks mad shit abt snowden.” At approximately 5:19 p.m., EST, LIVERMAN asked CRACKA, “if you come across anything related to [Victim 3’s spouse] let me know,” and “[Victim 3’s

spouse] needs to getrekt.”²¹ Approximately eleven minutes later, LIVERMAN told CRACKA that “bashtien wants to phonebomb the shitt outta [Victim 3’s spouse].” “Bashtien” is one of LIVERMAN’s online identities that he used to obfuscate his true identity. After CRACKA told LIVERMAN that he had obtained a purported address for Victim 3’s spouse, LIVERMAN stated “I wish [sic] had [Victim 3’s spouse’s] cell,” and noted that “bashtien rocked [Victim 2’s] cell hard … 720 voicemail threats and like 1000 goatse²² sms image messages.” CRACKA subsequently told LIVERMAN that he had obtained Victim 3’s spouse’s Verizon ISP account number and was attempting to obtain the 4-digit PIN to their account.

42. Records obtained from Verizon include voice recordings of several social engineering calls that CRACKA made on or about December 10, 2015 to Verizon regarding Victim 3’s Verizon account. In the calls, CRACKA impersonated both a Verizon employee and Victim 3 (the account holder).

43. During a December 12, 2015, Jabber chat session, at approximately 1:57 p.m., EST, CRACKA sent LIVERMAN a LightShot link that appeared to be a Verizon web page with the words, “Please wait while we retrieve your account information.” LIVERMAN responded by asking if CRACKA had obtained access to Victim 3’s Verizon account. CRACKA replied that he was trying to see if he could access Victim 3’s spouse’s call logs and that he was having some issues logging into their Verizon account. CRACKA stated, “the account keeps fucking up for me. sometimes it lets me log in sometimes it doesn’t.” At approximately 2:02 p.m., EST, CRACKA stated, “i’ll

²¹ “Rekt” is Internet slang for “wrecked.”

²² “Goatse” refers to a lewd image of a naked man.

try logging in now. it only lets me log in through tor lol²³. i always log in through tor on jacked accounts anyways.” CRACKA then asked LIVERMAN if LIVERMAN wanted to try logging into Victim 3’s Verizon account. LIVERMAN replied, “yes :D.” LIVERMAN then told CRACKA to call Victim 3’s spouse’s cellular telephone number. At approximately 2:19 p.m., EST, LIVERMAN stated that he couldn’t place the call himself because “i dont have any voip and down to my last burner.”²⁴ Over the next few days, CRACKA placed several calls to Victim 3’s spouse’s cellular telephone, as well as Victim 3’s home telephone. Call records show that on or about December 12, 2015, telephone number (213) 204-XXXX placed an approximately 11-second call to Victim 3’s cellular telephone. Records from a Bitcoin exchange revealed that telephone number (213) 204-XXXX is associated with an account under the name of “Joseph Markowicz” with a registration email address of d3f4ult[@]protonmail.ch. As described in earlier paragraphs, Joseph Markowicz is the vanity name for LIVERMAN’s Facebook account. Moreover, records for Twitter account @_D3F4ULT show the same registration email address of d3f4ult[@]protonmail.ch that was used to register the same Bitcoin account.

44. During the same December 12, 2015 Jabber chat session, LIVERMAN and CRACKA discussed ways to deface the sign-on page for Victim 3’s online Verizon account. CRACKA sent LIVERMAN two versions of a defaced image for the account. LIVERMAN and CRACKA also discussed how they should use Twitter to taunt Victim 3. Ultimately they decided to impersonate Edward Snowden to taunt Victim 3 on

²³ Tor is an encrypted network that can route your traffic through relays, making the traffic appear to come from Tor exit nodes.

²⁴ “VoIP” stands for Voiceover Internet Protocol. VoIP is a technology that allows a user to make voice calls over the Internet. Your affiant believes that the reference to “burner” is a reference to a burner mobile application that allows smartphone users to have temporary, disposable telephone numbers.

Twitter. At approximately 4:56 p.m., EST, after discussing the exact text with CRACKA, LIVERMAN (using Twitter screen name @BASHTIEN_) publicly tweeted, “dis is @Snowden, I heard u talkin shit [Twitter handle associated to Victim 3’s spouse] so i tok ur acc bish!” The post included a defaced image of a Verizon account’s sign-in page that included reference to three Twitter users, “cracka_d3f4ult_bashtien_2015” below the Verizon site key image of a snow man.

45. During the same December 12, 2015 Jabber chat session, CRACKA provided LIVERMAN with the login credentials for Victim 3’s online Verizon account. A contemporaneous Bandicam recording made by LIVERMAN showed multiple attempts by LIVERMAN on or about December 12, 2015 between 3:23 p.m., EST, and 3:44 p.m., EST, to access Victim 3’s online Verizon account. The contemporaneous video recording also showed LIVERMAN coordinating his efforts to access Victim 3’s online Verizon account with CRACKA during the December 12, 2015 Jabber chat session described above.

The Conspiracy Targets Victim 4

46. During a December 18, 2015 Jabber chat session, at approximately 8:16 p.m., EST, CRACKA sent LIVERMAN a news article about Victim 4 with the comment “[Victim 4’s] getting hacked.” Victim 4 resides in the Eastern District of Virginia. LIVERMAN responded less than a minute later, “fuck yeah plz do.” LIVERMAN stated that Victim 4 probably had some secrets. At approximately 8:34 p.m., EST, CRACKA stated, “i’ll see what i can do :3.” At approximately 9:21 p.m., EST, LIVERMAN asked CRACKA if he had discovered Victim 4’s cellular telephone number yet because, “id loooove to phonebomb [Victim 4’s] voicemail … and sms spam.”

47. During a December 19, 2015, Jabber chat session, at approximately 3:27 p.m., EST, CRACKA told LIVERMAN that he had obtained access to Victim 4's online Comcast account, a fact which is supported by Comcast records. Less than one minute later, LIVERMAN responded, "roger that, set off the explosives." Over the next few hours, CRACKA and LIVERMAN discussed different ways of harassing Victim 4 using the information obtained from CRACKA's access to Victim 4's online Comcast account. CRACKA sent LIVERMAN screenshots of his activities while in Victim 4's online Comcast account, including evidence that CRACKA harassed Victim 4 by altering the settings for the Comcast account at Victim 4's home located in the Eastern District of Virginia, such as resetting the passcode to Victim 4's voicemail, remotely playing movies on Victim 4's "family room" cable box, and renaming Victim 4's cable boxes to derogatory statements about Victim 4. LIVERMAN instructed CRACKA to send him Victim 4's call logs via Crytobin.

48. Call logs for Victim 4's home Comcast account was found on one of LIVERMAN's hard drives.

49. On or about December 19, 2015, Victim 4 received a notification from Comcast that the password to Victim 4's online Comcast account had been changed. Victim 4 also received a telephone call that was harassing in nature allegedly from CRACKA on or about December 19, 2015.

50. During a December 24, 2015, Jabber chat session, among other things, CRACKA and LIVERMAN chatted about CRACKA's new Twitter account, @DICKREJECT. At approximately 5:56 p.m., EST, CRACKA asked LIVERMAN if he

should release Victim 4's call logs. Within a minute, LIVERMAN responded, "ayyyyyyyyyy fuck yes" and "early christmas."

51. On or about December 24, 2015, at approximately 5:59 p.m., EST, CRACKA (using Twitter screen name @DICKREJECT) publicly tweeted, "Merry Christmas @[Victim 4's law enforcement agency] [Victim 4] Call Logs cryptobin.org/XXXXXXXXX Password is lol." This Cryptobin link contained several pages worth of Victim 4's call records from Victim 4's home telephone number located in the Eastern District of Virginia from on or about September 20, 2015 to on or about December 16, 2015.

The Conspiracy Targets Victim 5

52. During a December 27, 2015, Jabber chat session, at approximately 9:29 a.m., EST, CRACKA told LIVERMAN that he would target Victim 5's company. LIVERMAN asked "why them?" About 30 minutes later, CRACKA answered, "im targeting them because they supply gov," to which LIVERMAN responded "niice." CRACKA first targeted the Facebook page belonging to Victim 5's spouse. Facebook records revealed that the Facebook account belonging to Victim 5's spouse was accessed from a Tor IP address on or about December 27, 2015, at approximately 2:22 p.m., EST. At approximately 2:35 p.m., EST, CRACKA shared a LightShot link of a draft post from Victim 5's spouse's Facebook page that read "Jacked by Cracka." CRACKA then found a January 1, 2016 restaurant reservation for two at a restaurant near Victim 5's residence. At approximately 3:17 p.m., EST, LIVERMAN told CRACKA to "cancel that shit," which CRACKA replied, "i already cancelled it." LIVERMAN and CRACKA then discussed different ways of harassing Victim 5 and Victim 5's spouse. LIVERMAN and

CRACKA then coordinated via Jabber chat a conversation they also had via Facebook as Victim 5's spouse and Joseph Markowicz, an account controlled by LIVERMAN.

53. A screenshot of a Facebook Friend Request from LIVERMAN to the compromised account of Victim 5's spouse's Facebook account, which was compromised by CRACKA, was found in one of LIVERMAN's computer hard drives.

54. On or about December 27, 2015, at approximately 4:09 p.m., EST, CRACKA (using Twitter screen name @DICKREJECT) publicly tweeted, "There seems to be some strange posts coming from [Victim 5's spouse's] facebook account." This tweet included a partial screenshot of purported Facebook messages from Victim 5's spouse. For example, one of these purported Facebook messages stated, "The US government funds Israel so they can kill innocent people in Palestine. The US government and the Israel government are the real terrorists. Bush Did 911. Jet fuel doesn't melt steel beams." At approximately 6:09 p.m., EST, CRACKA told LIVERMAN by way of Jabber chat that he "took [Victim 5's] linkedin too lmao."

55. On or about December 28, 2015, at approximately 5:23 a.m., EST, @DICKREJECT publicly tweeted, "this ceo is a [derogatory comment] hahahaha." Less than twenty minutes later, @DICKREJECT publicly tweeted, "whats happened to [Victim 5's] LinkedIn? LinkedIn.com/[Victim 5's name]." This tweet included a screenshot of Victim 5's defaced LinkedIn page that included, "recently fucking rekt by cracka." Later that same day, LIVERMAN (using Twitter screen name @_D3F4ULT) re-tweeted @DICKREJECT's tweet about Victim 5's defaced LinkedIn page. LinkedIn records revealed that Victim 5's LinkedIn page was accessed from Tor IP addresses on or about December 28, 2015.

56. Later on December 28, 2015, LIVERMAN and CRACKA, by way of Jabber, continued to chat about Victim 5's spouse's Facebook account. At approximately 7:56 p.m., EST, LIVERMAN stated, "awwww [Victim 5's spouse] defriended me." CRACKA replied, "[Victim 5's spouse] must've seen our fucking facebook messages." At approximately 8:07 p.m., EST, LIVERMAN told CRACKA "i just called [Victim 5's spouse] a whistler blower on twitter hhhhhhhhhhhhhhhhhhhhhhhhh." On or about December 28, 2015, at approximately 8:04 p.m., EST, LIVERMAN (using Twitter screen name @_D3F4ULT) made the following public tweet: "shouts to [Victim 5's spouse] for showing #AnonSec that love & becoming a whistleblower!" This tweet included a screenshot that appears to show Victim 5's spouse's compromised Facebook page. Less than twenty minutes later, approximately 8:20 p.m., EST, @DICKREJECT tweeted a hashtag for FreePalestine. This tweet included what appears to be a screenshot of Victim 5's spouse's defaced Facebook message response to a friend's messages that read, "If you are a friend of [Victim 5's spouse], please be aware that [his/her] account has been hacked and ignore any offensive posts. They are not from [Victim 5's spouse]." The purported response from Victim 5's spouse reads: "[Derogatory term] HOW IS SAYING FREE PALESTINE OFFENSIVE?! [Derogatory comment] FREE PALESTINE FUCK ISRAEL FREE PALESTINE FUCK ISRAEL."

***The Conspiracy Releases Information About Miami-Area Police Officers
Obtained from the LEEP Computer System***

57. On or about January 21, 2016, LIVERMAN (using Twitter screen name @BASHTIEN_) publicly tweeted links to two sites that contained information on more than 80 police officers/employees of several Miami-area law enforcement agencies. The data contained names, work phone numbers, emails, and titles of more than 80

officers/employees of several Miami-area law enforcement agencies. The data was obtained from the LEEP computer system in or about November 2015 when a member of the Conspiracy unlawfully accessed the LEEP computer system.

The Conspiracy “Swats” the Palm Beach Sheriff’s Office

58. During a January 16, 2016, Jabber chat session, CRACKA and LIVERMAN discussed “swatting” a police department. Below is a partial transcript of that Jabber chat session:

SENDER	TIME	TEXT
CRACKA	3:46:11 PM	im gonna swat a police department
CRACKA	3:47:03 PM	yolo
CRACKA	3:47:04 PM	lmao
CRACKA	3:48:49 PM	what shall i say
LIVERMAN	3:49:10 PM	ayyyyyyyy yolo fuck it
CRACKA	3:49:23 PM	what shall i say tho
LIVERMAN	3:49:31 PM	hopefully they will have a shootout and kill eachother
CRACKA	3:49:32 PM	i got bombs in the building?
CRACKA	3:49:36 PM	LOL yeee
CRACKA	3:49:49 PM	shall i say i got bombs in the building?
LIVERMAN	3:51:25 PM	yeaaa that usually works
LIVERMAN	3:51:33 PM	nano thermite hhhhhhhh
CRACKA	3:51:54 PM	LOL aight im doing it now
CRACKA	3:52:14 PM	im nervous as fuck
CRACKA	3:54:08 PM	IM DOING IT
	...	
CRACKA	3:59:29 PM	i told them i had bombs at their building

In the following minutes, CRACKA shared several links to tweets and news articles about an unfolding bomb threat and building evacuation at the Palm Beach County Sheriff’s Office’s (“PBSO”) Belle Glade administrative building in Belle Glade, Florida. On or about January 16, 2016, CRACKA (using Twitter screen name @DICKREJECT) publicly tweeted about the swatting event several times, including tagging LIVERMAN

(@BASHTIEN_) with emoticons of a smiley face and a heart. In one of the tweets, CRACKA said, “i love the chaos 8.”

59. According to records and an audio recording maintained by the PBSO, on or about January 16, 2015, at approximately 3:54 p.m., EST, I believe that CRACKA, contacted the PBSO non-emergency telephone line. He told the dispatcher that “I have some bombs.” He told the dispatcher that the bombs were at the Belle Glade Police Department, provided a fake name, and stated that he was calling from a phone that he found and that he was in a white truck. He later stated that the bombs were actually at the location of a police-involved shooting that occurred earlier that day which garnered national media coverage. The call lasted approximately five minutes.

60. Moreover, during the January 16, 2016 Jabber chat between CRACKA and LIVERMAN, CRACKA described his “swatting” call with the PBSO. CRACKA related, “they asked me where i put them and i said i don’t know.” LIVERMAN replied, “imagine all the ppl running around rn. thinking there is a bomb in the building.” CRACKA replied, “hhahahaa. I GOT KIDS.” CRACKA related, “i said i was in a white truck. dude legit she asked me where i put them in the police department or the sheriff’s and i said hold on and searched up where the shooting happened.”

61. In response to this call, the PBSO dispatched multiple police officers who evacuated the Belle Glade administrative building. No explosive devices were found during a search of the building.

62. LIVERMAN had a file named “cwa_target:” on one of his hard drives. This list contained the names of 14 victims to include the names of the Victims described herein.

The Conspiracy Targets the DOJ's Civil Division's CIMS Application

63. On or about January 30, 2016, at approximately 1:39 p.m., EST, a member of the Conspiracy using Twitter screen name @DOTGOVS, publicly tweeted, "Oh.." This tweet included a screenshot of the DOJ's Civil Division, Office of Management Information, Case Information Management System's ("CIMS") landing page. The email address that was used to register the @DOTGOVS account was the same email address that was used to register the @PHPHAX account.

64. On or about February 03, 2016, CRACKA and LIVERMAN engaged in Jabber chat, wherein CRACKA related, "...i owned the entire DOJ. like, all DOJ agencies so fbi, dea, Interpol, dhs. i'm sitting here with 20k fbi employee names, country, email, phone number, title. i have access to a DOJ computer. CRACKA provided LIVERMAN with some screenshots to include a screenshot of what appears to be the main internal DOJ Civil Division landing page. LIVERMAN stored the DOJ screenshots on his computer.

65. On or about January 30, 2016, at approximately 4:40 p.m., EST, @DOTGOVS publicly tweeted, "9,000 @DHSgov employees. :(." This tweet included a partial redacted screenshot containing names and dhs.gov domain names.

66. On or about January 30, 2016, at approximately 5:13 p.m., EST, @DOTGOVS publicly tweeted, "Why do we have 20,000 @FBI employees: names, phone numbers, countries, and emails? Including ones abroad :)."

67. According to the DOJ Justice Security Operations Center ("JSOC"), CIMS is a DOJ Civil Division internal only application that is not publically accessible via the Internet. A JSOC analysis determined that a member of the Conspiracy had social

engineered the DOJ Civil Division help desk and then obtained access to an identified DOJ contract employee's credentials. On multiple occasions between on or about January 27, 2016 and on or about February 2, 2016, a member of the Conspiracy used the employee's credentials to fully access the CIMS application and DOJ systems.

68. On or about February 7, 2016, at approximately 2:24 p.m., EST, @DOTGOVS publicly tweeted, "well folks, it looks like @TheJusticeDept has finally realized their computer has been breached after 1 week."

69. On or about February 7, 2016, at approximately 6:57 p.m., EST, @DOTGOVS publicly tweeted, "ALL DHS.GOV EMPLOYEES (9,000) NAMES, TITLES, PHONE NUMBER, STATE, EMAIL cryptobin.org/XXXXXXXX #FreePalestine pass [password] is lol." The [cryptobin.org](http://cryptobin.org/XXXXXXXX) link in this tweet contained approximately 9,000 DHS employee names and their respective titles, telephone numbers, and email addresses in alphabetical order from A to Z.

70. On or about February 7, 2016, at approximately 9:02 p.m., EST, @DOTGOVS publicly tweeted, "Tomorrow we shall release 20,000 FBI employees data, including ones outside the US. :) #FreePalestine."

71. On or about February 7, 2016, at approximately 10:26 p.m., EST, @DOTGOVS publicly tweeted, "Ahoy there, follow @IncursioSubter and wait for the 20,000 FBI employee data drop, maybe it'll get dropped early ;)."

72. On or about February 8, 2016, at approximately 3:43 p.m., EST, @DOTGOVS publicly tweeted, "20,000 FBI EMPLOYEES NAMES, TITLES, PHONE NUMBERS, EMAILS, COUNTRY cryptobin.org/XXXXXXXX password is lol #FreePalestine." The [cryptobin.org](http://cryptobin.org/XXXXXXXX) link in this tweet contained approximately 22,000

FBI employee names and their respective titles, telephone numbers, and email addresses in alphabetical order from A to J.

73. The entire 20,000 FBI employee information and the 9,000 DHS employee information were stored on LIVERMAN's computer.

74. On or about February 9, 2016, the U.K. authorities searched CRACKA's residence and conducted other law enforcement action.

75. On or about February 10, 2016, at approximately 9:26 a.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, "Either the servers at cryptobin were overwhelmed or the feds shut it down. I'm voting for the latter."

76. On or about February 10, 2016, at approximately 9:31 a.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, "Archived: indybay.org/uploads/2016/0... [@DotGovs.](http://indybay.org/uploads/2016/0...)" These two indybay.org upload links contained the thousands of FBI and DHS employee names, telephone numbers, and email addresses that were allegedly stolen from DOJ's CIMS application by way of unauthorized access as described above.

77. On or about February 11, 2016, at approximately 10:33 a.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, "Before publishing any of the leaks from @dotgovs on pastebin, make sure you're using a VPN or public wifi. @pastebin is known for snitching."

78. On or about February 11, 2016, at approximately 11:54 a.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, "Cryptobin went down roughly the same time a member of @dotgovs was "arrested." Do you still think it's coincidental?"

79. On or about February 11, 2016, at approximately 3:14 p.m., EST, BOGGS (using Twitter screen name @INCURSIOSUBTER) publicly tweeted, “@DotGovs suspended. Follow our backup: @Dotgovz_.”

80. On or about February 12, 2016, at approximately 8:31 a.m., EST, @DOTGOVZ_ publicly tweeted, “ghostbin.com/paste/gd5rd/raw Leak directory from most of our leaks. Will be updated in future !!! (Not every leak is there).” This ghostbin.com paste contains URLs to the thousands of FBI and DHS employee names, telephone numbers, and email addresses that were allegedly stolen from DOJ’s CIMS application by way of unauthorized access. Twitter records for @DOTGOVZ_ account appears to show that CUBED had access to the @DOTGOVZ_ account. Specifically, on or about February 11, 2016, at approximately 3:11 p.m., EST, a Twitter user sent a DM to @DOTGOVZ_ and asked if he was @Fruityhax. A few minutes later, @DOTGOVZ_ replied, “Yeh.” At approximately 3:24 p.m., EST, @DOTGOVZ_ sent a DM to another Twitter user that read, “ill message you on my fruityhax account if you want.” On or about February 12, 2016, at approximately 8:49 a.m., EST, @DOTGOVZ_ sent a DM to another Twitter user that CRACKA, “was arrested by [Law Enforcement Agency in the UK].”

CONCLUSION

81. Based on the foregoing, I believe that there is probable cause to support the attached complaint and associated arrest warrants for ANDREW OTTO BOGGS and JUSTIN GRAY LIVERMAN.



BJ Kang
Special Agent
Federal Bureau of Investigation

Reviewed by: AUSA Jay V. Prabhu
AUSA Maya Song
SAUSA (LT) Joseph V. Longobardo

Subscribed and sworn to before me
on September 2, 2016:

/s/ 

Michael S. Nachmanoff
United States Magistrate Judge
Honorable Michael S. Nachmanoff
United States Magistrate Judge

Alexandria, Virginia